CHORUS MART

ROUTER KNX/IP - KNX SECURE - IP20 - 1 MODULO DIN

GW A9710

Manuale tecnico

Contents

1 Introduzione

Il dispositivo compatto consente l'inoltro di telegrammi tra diverse linee tramite una LAN (IP) come backbone veloce. Il dispositivo funge anche da interfaccia di programmazione tra un PC e il bus KNX (ad es. per la programmazione ETS).

Il dispositivo supporta KNX Security. L'opzione può essere attivata nell'ETS. Come router sicuro, il dispositivo consente l'accoppiamento di comunicazioni non protette su una linea KNX TP con una dorsale IP sicura.

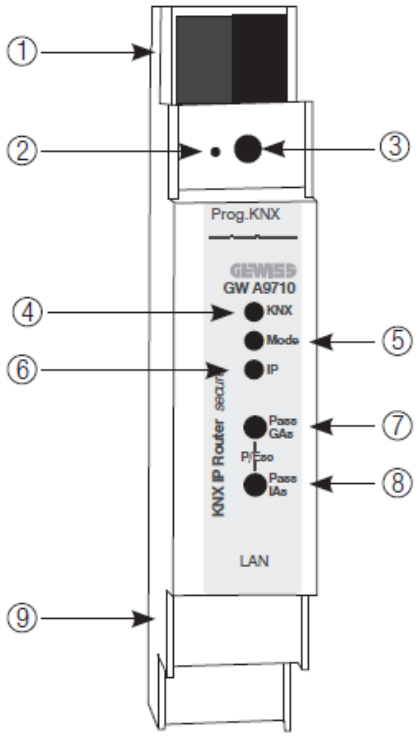
KNX Security impedisce anche l'accesso non autorizzato alla funzione di interfaccia (tunneling).

L'indirizzo IP può essere assegnato tramite DHCP o tramite la configurazione ETS. Il dispositivo funziona secondo la specifica KNXnet/IP utilizzando core, gestione dei dispositivi, tunneling e routing.

Il dispositivo dispone di una tabella di filtri estesa per i gruppi principali 0..31 e può bufferizzare fino a 150 telegrammi. L'alimentazione viene fornita tramite il bus KNX.

2 Installazione

Il dispositivo è progettato per essere installato su una guida DIN con una larghezza di 1 unità (18 mm). È dotato dei seguenti comandi e display:



1. **Connettore bus KNX**
2. **LED di programmazione**
3. **Pulsante per modalità di programmazione**
4. **LED KNX (multicolore)**
5. **LED Mode (multicolore)**
6. **LED IP (multicolore)**
7. **Pulsante Pass GAs**
8. **Pulsante Pass IAs**
9. **Connettore LAN**

Il dispositivo è alimentato dal bus KNX. Non è necessario un alimentatore esterno

In assenza di tensione sul bus, il dispositivo non funziona.

2.1 Modalità di programmazione KNX

La modalità di programmazione KNX viene attivata/disattivata premendo il pulsante di programmazione KNX incassato ❸ oppure premendo contemporaneamente i pulsanti ❼ e ❽.

2.2 Indicatore di stato

Il LED KNX ❹ si illumina di verde se il dispositivo è alimentato correttamente dal bus KNX. Questo LED indica il traffico di telegrammi sul bus KNX lampeggiando.

I guasti di comunicazione (ad es. ripetizioni di telegrammi o frammenti di telegrammi) sono indicati da un breve cambiamento del colore del LED in rosso.

Panoramica delle diverse indicazioni del LED KNX ❹:

LED Status	Significato
LED verde	Tensione bus KNX disponibile.
LED verde lampeggiante	Traffico telegrammi sul bus KNX.
LED rosso lampeggiante	Errori di comunicazione sul bus KNX.

Il LED IP ❻ si accende quando è attivo un collegamento Ethernet. Questo LED è verde se il dispositivo ha impostazioni IP valide (indirizzo IP, sottorete e gateway). Con impostazioni IP non valide o inesistenti, il LED è rosso. Questo vale anche se, ad esempio, il dispositivo non ha ancora ricevuto le impostazioni IP da un server DHCP.

Questo LED indica il traffico di telegrammi IP lampeggiando.

Panoramica delle diverse indicazioni del LED IP ❻:

LED Status	Significato
LED verde	Il dispositivo ha un collegamento Ethernet attivo e impostazioni IP valide.
LED rosso	Il dispositivo ha un collegamento Ethernet attivo e impostazioni IP non valide o non ha ancora ricevuto le impostazioni IP da un server DHCP.
LED verde lampeggiante	Traffico di telegrammi IP

A scopo di test (ad esempio durante la messa in servizio), le impostazioni di routing configurate (filtro o blocco) possono essere bypassate tramite comando manuale.

Con il pulsante Pass GAs ❼ è possibile attivare l'inoltro dei telegrammi indirizzati al gruppo.

Con il pulsante Pass IAs ❽ è possibile attivare l'inoltro dei telegrammi indirizzati individualmente.

Ciò viene visualizzato con un singolo lampeggio del LED Mode ❺ (arancione). Se entrambe le modalità sono attivate, il LED Mode ❺ lampeggia due volte.

Premendo nuovamente il pulsante Pass GAs ❼ o il pulsante Pass IAs ❽ è possibile selezionare e deselezionare queste impostazioni a piacere. Tramite la funzione Escape (Esc) è possibile interrompere il funzionamento manuale premendo contemporaneamente i pulsanti Pass GAs ❼ e Pass IAs ❽.

Se né la modalità di programmazione né la modalità manuale sono attive, il LED ❺ può visualizzare errori di configurazione.

Panoramica delle diverse indicazioni del LED Mode ❺:

LED Status	**Significato**
LED verde	Il dispositivo funziona in modalità operativa standard.
LED rosso	La modalità di programmazione è attiva
LED lampeggiante 1x arancione	La modalità di programmazione non è attiva. Il funzionamento manuale è attivo. Inoltro IA o GA
LED lampeggiante 2x arancione	La modalità di programmazione non è attiva. Il funzionamento manuale è attivo. Inoltro IA e GA
LED lampeggiante rosso	La modalità di programmazione non è attiva. Il funzionamento manuale non è attivo. Il dispositivo non è caricato correttamente, ad es. dopo un download interrotto.

3 Ripristino delle impostazioni predefinite di fabbrica

È possibile ripristinare le impostazioni predefinite di fabbrica del dispositivo:

- Scollegare il connettore KNX Bus ❶ dal dispositivo
- Premere il pulsante di programmazione KNX ❸ e tenerlo premuto
- Ricollegare il connettore KNX Bus ❶ al dispositivo
- Tenere premuto il pulsante di programmazione KNX ❸ per almeno altri 6 secondi
- Un breve lampeggiamento di tutti i LED (❷❹❺❻) indica che il ripristino delle impostazioni predefinite di fabbrica del dispositivo è stato eseguito correttamente.

3.1 Impostazioni predefinite di fabbrica

La seguente configurazione è impostata di fabbrica:

Indirizzo individuale del dispositivo: 15.15.0

Numero di connessioni tunneling KNXnet/IP configurate: 1

Indirizzo individuale della connessione tunneling: 15.15.240

Assegnazione indirizzo IP: DHCP

Chiave iniziale (FDSK) attiva

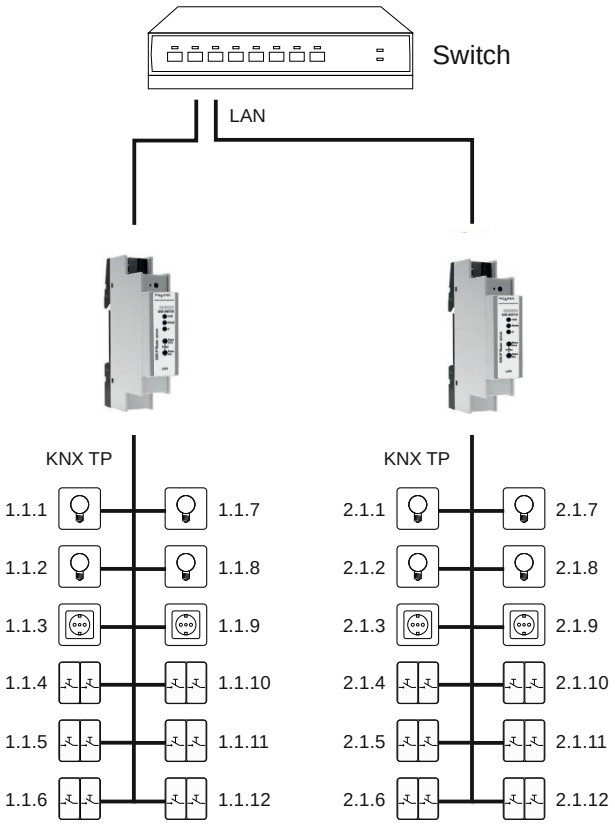
Modalità di sicurezza non attiva

4 Funzione di accoppiatore (KNXnet/IP Routing)

Il dispositivo funziona come accoppiatore di linea o backbone. In entrambi i casi, la LAN (IP) viene utilizzata come backbone.

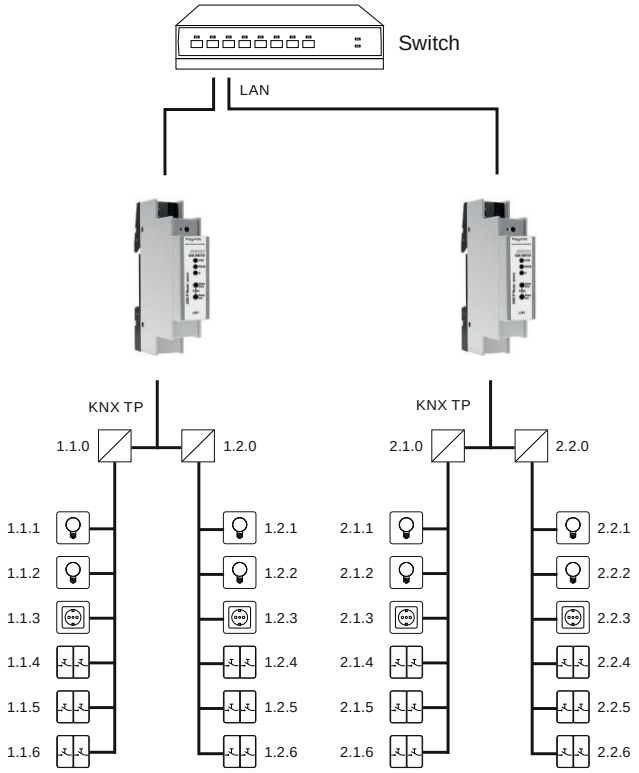
La tabella seguente mostra le possibilità di applicazione del router IP KNX rispetto alla topologia classica:

	Topologia classica (senza IP)	**Accoppiamento IP di aree (accoppiatore area IP)**	**Accoppiamento IP di linee (accoppiatore di linea IP)**
Area (Backbone)	TP	IP	IP
Accoppiamento	KNX Line Coupler (max. 15 Pcs.)	KNX IP Router (max. 15 Pcs.)	Direttamente tramite Switch LAN
Linea principale	TP	TP	IP
Accoppiamento	KNX Line Coupler (max. 15x15 Pcs.)	KNX Line Coupler (max. 15x15 Pcs.)	KNX IP Router (max. 225 Pcs..)
Linea	TP	TP	TP



Router IP KNX come accoppiatore di linea

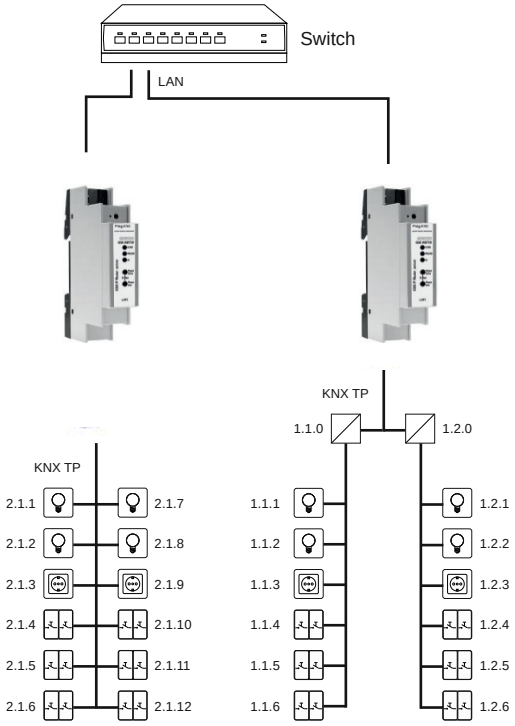
L'indirizzo individuale assegnato al dispositivo determina se il dispositivo funziona come accoppiatore di linea o di area. Se l'indirizzo individuale è nella forma x.y.0 (x, y: 1..15), il router funziona come accoppiatore di linea. Se è nella forma x.0.0 (x: 1..15), il router funge da accoppiatore backbone.



Router IP KNX come accoppiatore di area

Se il dispositivo viene utilizzato come accoppiatore di area (x.0.0), nella topologia sottostante non deve essere presente alcun router IP KNX. Ad esempio, se un router IP KNX ha l'indirizzo individuale 1.0.0, non deve essere presente alcun router IP KNX con l'indirizzo 1.1.0.

Se il dispositivo viene utilizzato come accoppiatore di linea (x.y.0), nella topologia al di sopra di esso non deve essere presente un router IP KNX. Ad esempio, se un router IP KNX ha l'indirizzo individuale 1.1.0, non deve essere presente alcun router IP KNX con l'indirizzo 1.0.0.



Router IP KNX come accoppiatore di area e linea

Il router IP KNX dispone di una tabella di filtri e contribuisce quindi a ridurre il carico del bus. La tabella di filtri (8 kB) supporta l'intervallo di indirizzi di gruppo esteso (gruppi principali 0...31) e viene generata automaticamente dall'ETS.
A causa della differenza di velocità tra Ethernet (10/100 MBit/s) e KNX TP (9,6 kBit/s), su IP è possibile trasmettere un numero molto maggiore di telegrammi. Se vengono trasmessi più telegrammi consecutivi per la stessa linea, questi devono essere bufferizzati nel router per evitare la perdita di telegrammi. Il dispositivo dispone di una memoria per 150 telegrammi (da IP a KNX).

Funzione di accesso al bus (KNXnet/IP Tunneling)

Il dispositivo può essere utilizzato come interfaccia per KNX. È possibile accedere al bus KNX da qualsiasi punto della LAN. A tal fine, è necessario assegnare un indirizzo individuale aggiuntivo. Ciò è descritto nelle sezioni seguenti.

5 KNX Security

Lo standard KNX è stato ampliato con KNX Security per proteggere le installazioni KNX da accessi non autorizzati. KNX Security impedisce in modo affidabile il monitoraggio delle comunicazioni e la manipolazione del sistema.

La specifica per KNX Security distingue tra KNX IP Security e KNX Data Security. KNX IP Security protegge la comunicazione su IP, mentre su KNX TP la comunicazione rimane non crittografata. Pertanto, KNX IP Security può essere utilizzato anche in sistemi KNX esistenti e con dispositivi KNX TP non sicuri.

KNX Data Security descrive la crittografia a livello di telegramma. Ciò significa che anche i telegrammi sul bus a doppino intrecciato sono crittografati.

KNX IP Security per la funzione router

Il collegamento di singole linee KNX TP tramite IP è denominato KNX IP routing.
La comunicazione tra tutti i router KNX IP collegati avviene tramite multicast UDP.
La comunicazione di routing è crittografata con KNX IP Security.

Ciò significa che solo i dispositivi IP che conoscono la chiave possono decrittografare la comunicazione e inviare telegrammi validi. Un timestamp nel telegramma di routing garantisce che nessun telegramma registrato in precedenza possa essere riprodotto. Ciò impedisce il cosiddetto attacco di replay.

La chiave per la comunicazione di routing viene riassegnata da ETS per ogni installazione. Se per il routing viene utilizzata la sicurezza KNX IP, tutti i dispositivi KNX IP collegati devono supportare la sicurezza ed essere configurati di conseguenza.

Sicurezza KNX IP per la funzione di interfaccia

Quando si utilizza un router KNX IP come interfaccia per il bus, l'accesso all'installazione è possibile senza sicurezza per tutti i dispositivi che hanno accesso alla rete IP. Con la sicurezza KNX è richiesta una password. Per la trasmissione della password viene già stabilita una connessione sicura. Tutte le comunicazioni via IP sono crittografate e protette.

KNX Data Security per il dispositivo

Il dispositivo supporta anche KNX Data Security per proteggere il dispositivo da accessi non autorizzati dal bus KNX. Se il router KNX IP viene programmato tramite il bus KNX, ciò avviene con telegrammi crittografati.

I telegrammi crittografati sono più lunghi di quelli non crittografati utilizzati in precedenza. Per una programmazione sicura tramite il bus, è quindi necessario che l'interfaccia utilizzata (ad es. USB) e gli eventuali accoppiatori di linea intermedi supportino i cosiddetti frame lunghi KNX.

KNX Data Security per telegrammi di gruppo

I telegrammi provenienti dal bus che non indirizzano il router IP KNX come dispositivo vengono inoltrati o bloccati in base alle impostazioni del filtro (parametri e tabella dei filtri). Non importa se i telegrammi sono non crittografati o crittografati. L'inoltro avviene esclusivamente sulla base dell'indirizzo di destinazione. Le proprietà di sicurezza vengono verificate dal rispettivo destinatario.

La sicurezza dei dati KNX e la sicurezza IP KNX possono essere utilizzate in parallelo. In questo caso, ad esempio, un sensore KNX invierebbe al bus un telegramma di gruppo crittografato con la sicurezza dei dati KNX. In caso di inoltro tramite KNX IP con sicurezza IP KNX, il telegramma crittografato verrebbe nuovamente crittografato proprio come quelli non crittografati. Tutti i partecipanti a livello KNX IP che supportano KNX IP Security possono decodificare la crittografia IP, ma non la sicurezza dei dati. Pertanto, il telegramma proveniente dagli altri router KNX IP viene nuovamente trasmesso alla linea o alle linee di destinazione con KNX Data Security. Solo i dispositivi che conoscono la chiave utilizzata per la sicurezza dei dati possono interpretare il telegramma.

6 Impostazioni dell'interfaccia con ETS

All'interno dell'ETS, le interfacce KNX possono essere selezionate e configurate tramite il menu ETS “Interfacce bus”.

L'ETS può accedere ai router IP KNX configurati anche senza una voce nel database. Se la configurazione del router IP KNX non è conforme alle condizioni dell'installazione KNX, è necessario configurarlo tramite un progetto ETS. Per ulteriori informazioni, consultare la sezione relativa al database ETS.

Come impostazione predefinita di fabbrica, l'assegnazione dell'indirizzo IP è impostata su “automaticamente tramite DHCP” e quindi non sono necessarie ulteriori impostazioni. Per utilizzare questa funzione è necessario che nella LAN sia presente un server DHCP (ad esempio, molti router DSL hanno un server DHCP integrato).

Dopo aver collegato il router IP KNX alla LAN e al bus KNX, dovrebbe apparire automaticamente nell'ETS nel menu “Bus” sotto “Interfacce rilevate”.

Cliccando sull'interfaccia rilevata, questa viene selezionata come interfaccia corrente. Sul lato destro della finestra ETS vengono visualizzate tutte le informazioni specifiche e le opzioni della connessione.

Il nome del dispositivo indicato e l'“indirizzo individuale host” (indirizzo individuale del dispositivo) possono essere modificati all'interno del progetto ETS.

Come tutti i dispositivi KNX programmabili, anche il KNX IP Router dispone di un indirizzo individuale che può essere utilizzato per accedere al dispositivo. Questo viene utilizzato, ad esempio, dall'ETS durante il download sul KNX IP Router tramite il bus.

Per la funzione di interfaccia, il dispositivo contiene indirizzi individuali aggiuntivi che possono essere impostati nell'ETS. Quando un client (ad es. ETS) invia telegrammi al bus tramite il router IP KNX, questi contengono un indirizzo mittente come uno degli indirizzi aggiuntivi. Ogni indirizzo è associato a una connessione. In questo modo, i telegrammi di risposta possono essere trasmessi in modo chiaro al rispettivo client.

Gli indirizzi individuali aggiuntivi devono essere selezionati dall'intervallo di indirizzi della linea bus in cui è installata l'interfaccia e non possono essere utilizzati da un altro dispositivo.

Esempio:

Indirizzo dispositivo 1.1.0 (indirizzo all'interno della topologia ETS)
Connessione 1 1.1.240 (1° indirizzo aggiuntivo)
Connessione 2 1.1.241 (2° indirizzo aggiuntivo)
Connessione 3 1.1.242 (3° indirizzo aggiuntivo)
Connessione 4 1.1.243 (4° indirizzo aggiuntivo)
Connessione 5 1.1.244 (5° indirizzo aggiuntivo)
Connessione 6 1.1.245 (6° indirizzo aggiuntivo)

Connessione 7 1.1.246 (7° indirizzo aggiuntivo)
Connessione 8 1.1.247 (8° indirizzo aggiuntivo)

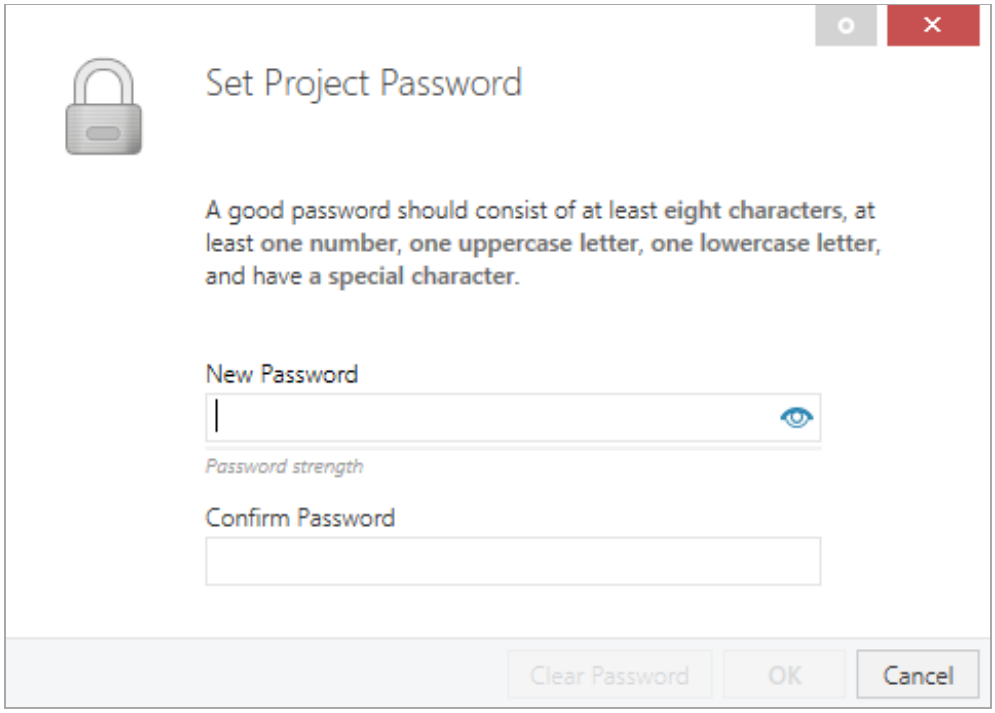
La sezione “Indirizzo individuale” consente di selezionare l'indirizzo KNX individuale della connessione KNXnet/IP Tunneling attualmente in uso.

L'indirizzo individuale del dispositivo KNX e gli indirizzi KNX individuali per le connessioni tunneling aggiuntive possono essere modificati all'interno del progetto ETS, dopo che il dispositivo è stato aggiunto al progetto.

7 ETS database

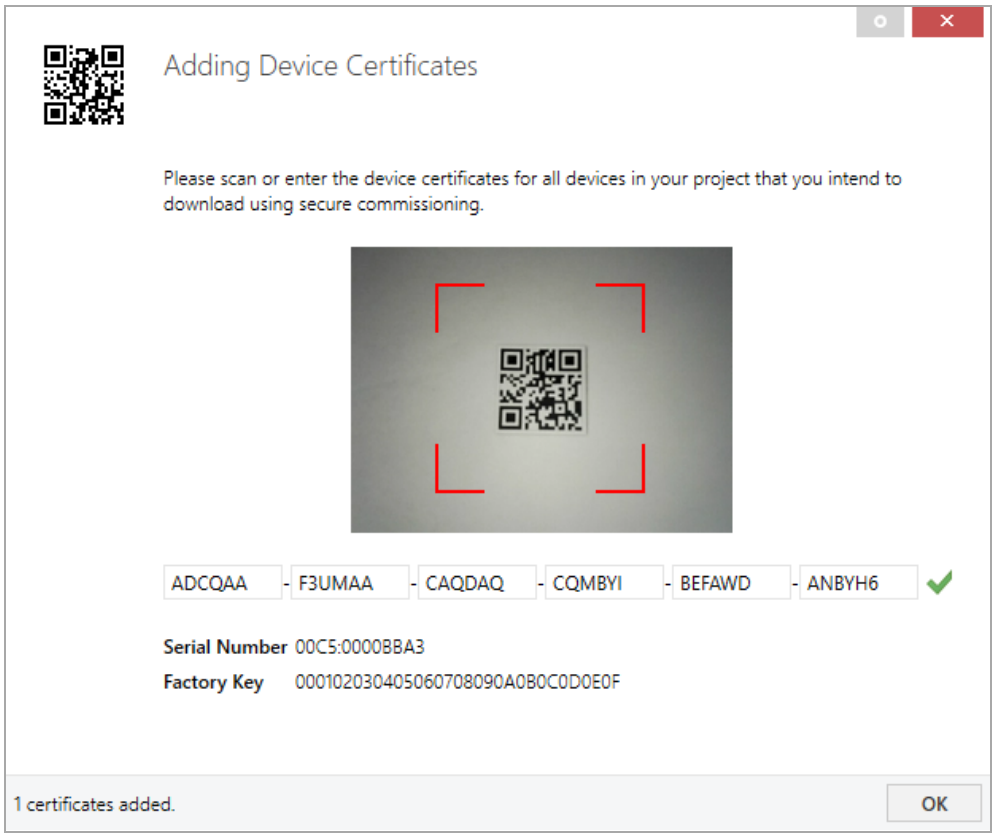
7.1 Secure commissioning

Se il primo prodotto viene inserito in un progetto con KNX Security, l'ETS richiede di inserire una password di progetto.



Questa password protegge il progetto ETS da accessi non autorizzati. Questa password non è una chiave utilizzata per la comunicazione KNX. L'inserimento della password può essere bypassato con “Annulla”, ma ciò non è consigliabile per motivi di sicurezza.

ETS richiede un certificato di dispositivo per ogni dispositivo con KNX Security creato in ETS. Questo certificato contiene il numero di serie del dispositivo e una chiave iniziale (FDSK = Factory Default Setup Key).



Il certificato viene stampato come testo sul dispositivo. Può anche essere comodamente scansionato dal codice QR stampato tramite una webcam.

L'elenco di tutti i certificati dei dispositivi può essere gestito nella finestra ETS Panoramica - Progetti - Sicurezza.

Questa chiave iniziale è necessaria per mettere in funzione un dispositivo in modo sicuro fin dall'inizio. Anche se il download ETS viene registrato da una terza parte, quest'ultima non avrà accesso ai dispositivi protetti in seguito. Durante il primo download sicuro, la chiave iniziale viene sostituita dall'ETS con una nuova chiave generata individualmente per ogni dispositivo. Ciò impedisce a persone o dispositivi che potrebbero conoscere la chiave iniziale di accedere al dispositivo. La chiave iniziale viene riattivata solo dopo un reset completo.

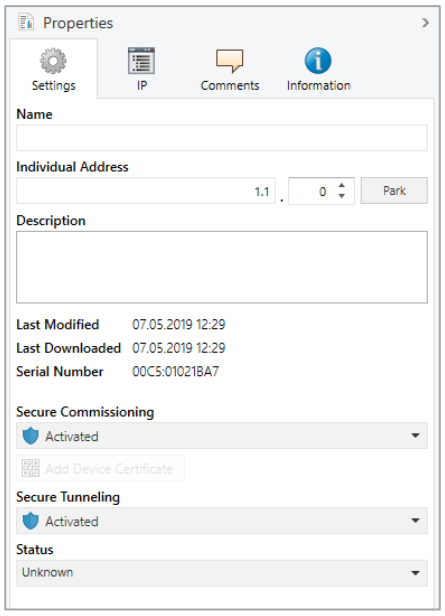
Il numero di serie nel certificato consente all'ETS di assegnare la chiave corretta a un dispositivo durante un download.

Nell'ETS, alcune impostazioni vengono visualizzate oltre alla finestra di dialogo dei parametri nella finestra di dialogo delle proprietà (sul bordo dello schermo). Qui è possibile effettuare le impostazioni IP. Gli indirizzi aggiuntivi per le connessioni dell'interfaccia vengono visualizzati nella vista topologica.

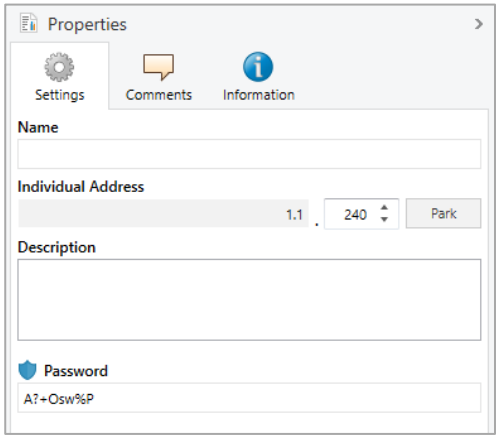
Ogni singolo indirizzo KNX può essere modificato cliccando sulla voce dell'elenco e digitando l'indirizzo desiderato nel campo di testo “Indirizzo individuale”. Se il campo di testo diventa rosso dopo aver inserito l'indirizzo, significa che l'indirizzo è già presente nel progetto ETS.

Assicurarsi che nessuno degli indirizzi sopra indicati sia già presente nell'installazione KNX.

Cliccando sulla voce Dispositivo nella vista topologica dei vostri progetti ETS, sul lato destro della finestra ETS apparirà una colonna informativa denominata “Proprietà”. Nella panoramica “Impostazioni” è possibile modificare il nome del dispositivo.



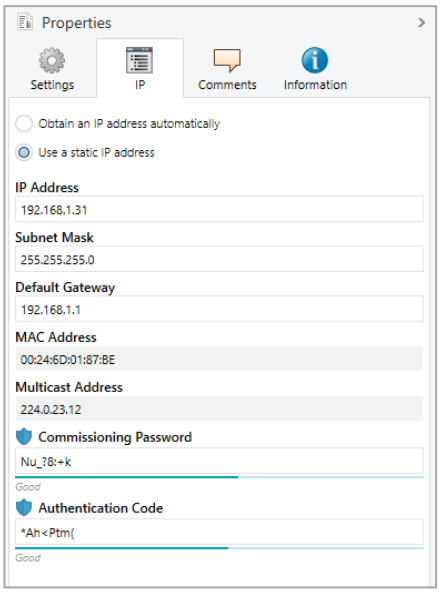
Se il tunneling sicuro è attivato, verrà creata automaticamente una password univoca per ogni tunnel. Queste password possono essere visualizzate nella panoramica “Impostazioni”, quando viene selezionato un tunnel.



Nella panoramica “IP” è possibile modificare le opzioni specifiche della rete IP del dispositivo.

Modificando l'impostazione “Ottieni automaticamente un indirizzo IP (tramite DHCP)” in “Usa un indirizzo IP statico” (indirizzo IP statico) è possibile impostare liberamente l'indirizzo IP, la subnet mask e il gateway predefinito.

Tutte le modifiche apportate nel menu delle proprietà diventano effettive solo dopo il download corretto dell'applicazione.



Indirizzo IP

Qui è possibile inserire l'indirizzo IP del dispositivo. Questo viene utilizzato per indirizzare il dispositivo tramite la rete IP (LAN). L'indirizzamento IP deve essere coordinato con l'amministratore della rete.

Subnet mask

Inserire qui la subnet mask. Il dispositivo utilizza i valori inseriti in questa maschera per determinare se nella rete locale è presente un partner di comunicazione. Se nella rete locale non è presente alcun partner, il dispositivo non invierà i telegrammi direttamente al partner, ma al gateway che instrada il telegramma.

Gateway predefinito

Inserire qui l'indirizzo IP del gateway, ad esempio il router DSL dell'installazione.

Indirizzo multicast di routing

Questo indirizzo viene utilizzato per il routing dei telegrammi su IP. L'indirizzo IP multicast 224.0.23.12 è stato riservato (KNXnet/IP) presso l'IANA (Internet Assigned Numbers Authority) per questo scopo. Se è necessario un indirizzo IP multicast diverso, questo deve essere compreso nell'intervallo da 239.0.0.0 a 239.255.255.255.

Esempio di assegnazione di indirizzi IP

Per accedere al dispositivo si utilizza un PC.

Indirizzo IP del PC: 192.168.1.30

Sottorete del PC: 255.255.255.0

Il dispositivo si trova nella stessa LAN, ovvero utilizza la stessa sottorete. La sottorete limita gli indirizzi IP che possono essere assegnati. In questo esempio, l'indirizzo IP del router IP KNX deve essere 192.168.1.xx, dove xx può essere un numero compreso tra 1 e 254 (ad eccezione di 30, che è già occupato dal PC client). È necessario assicurarsi che nessun indirizzo IP venga assegnato due volte.

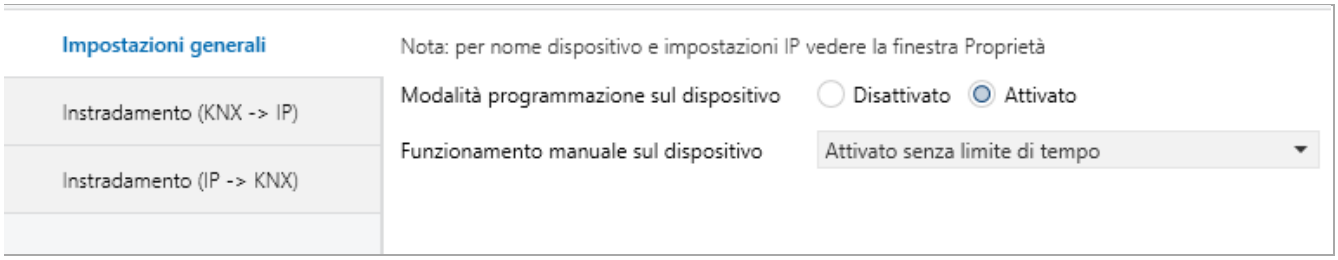
Indirizzo IP del router IP KNX 192.168.1.31

Sottorete del router IP KNX: 255.255.255.0

Accesso remoto

È possibile l'accesso remoto tramite Internet.

8 Impostazioni generali



Modalità di programmazione sul dispositivo

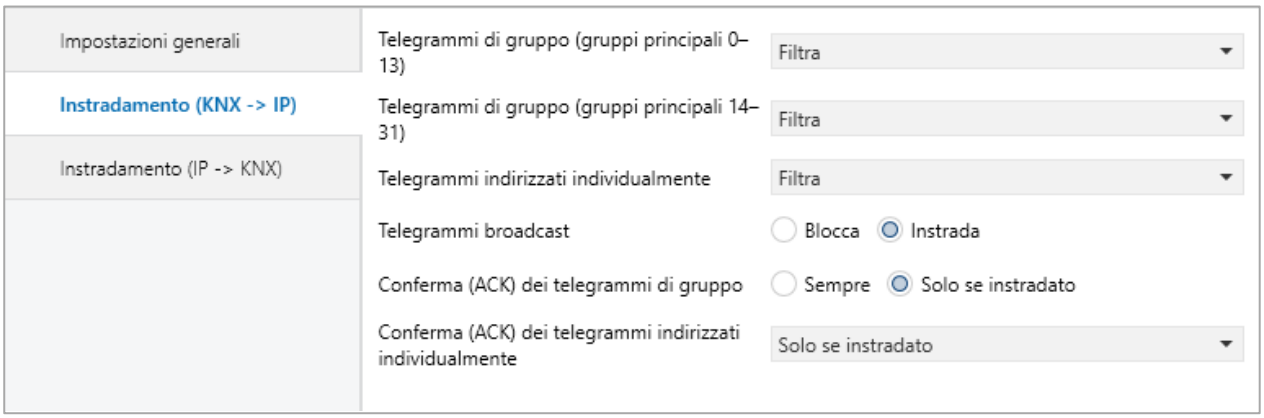
Oltre al normale pulsante di programmazione ❸, il dispositivo consente di attivare la modalità di programmazione sul dispositivo senza aprire il coperchio del quadro elettrico. La modalità di programmazione può essere attivata e disattivata premendo contemporaneamente entrambi i pulsanti ❼ e ❽.

Questa funzione può essere abilitata e disabilitata tramite il parametro “Modalità di programmazione sul pannello frontale del dispositivo”. Il pulsante di programmazione incassato ❸ (accanto al LED di programmazione ❷) è sempre abilitato e non è influenzato da questo parametro.

Funzionamento manuale sul dispositivo

Questo parametro imposta la durata della modalità manuale. Al termine, viene ripristinata la modalità di visualizzazione normale.

9 Instradamento (KNX -> IP)



Telegrammi di gruppo (gruppo principale da 0 a 13)

Blocca: Nessun telegramma di gruppo di questo gruppo principale viene instradato all'IP.

Instrada: Tutti i telegrammi di gruppo di questo gruppo principale vengono instradati all'IP indipendentemente dalla tabella dei filtri. Questa impostazione è solo a scopo di test.

Filtra: La tabella dei filtri viene utilizzata per verificare se il telegramma di gruppo ricevuto deve essere instradato all'IP.

Telegrammi di gruppo (gruppo principale da 14 a 31)

Blocca: Nessun telegramma di gruppo dei gruppi principali da 14 a 31 viene instradato all'IP.

Instrada: Tutti i telegrammi di gruppo dei gruppi principali da 14 a 31 vengono instradati all'IP.

Filtra: La tabella dei filtri viene utilizzata per verificare se il telegramma di gruppo ricevuto deve essere instradato all'IP.

Telegrammi indirizzati individualmente

Blocca: Nessun telegramma indirizzato individualmente viene instradato all'IP.

Instrada: Tutti i telegrammi indirizzati individualmente vengono instradati all'IP.

Filtra: L'indirizzo individuale viene utilizzato per verificare se il telegramma indirizzato individualmente ricevuto deve essere instradato all'IP.

Telegrammi broadcast

Blocca: Nessun telegramma broadcast ricevuto viene instradato all'IP.

Instrada: Tutti i telegrammi broadcast ricevuti vengono instradati all'IP.

Conferma (ACK) dei telegrammi di gruppo

Sempre: Viene generata una conferma per ogni telegramma di gruppo ricevuto (da KNX).

Solo se instradato: Viene generato un riconoscimento solo per i telegrammi di gruppo ricevuti (da KNX) se questi vengono instradati all'IP.

Conferma (ACK) dei telegrammi indirizzati individualmente

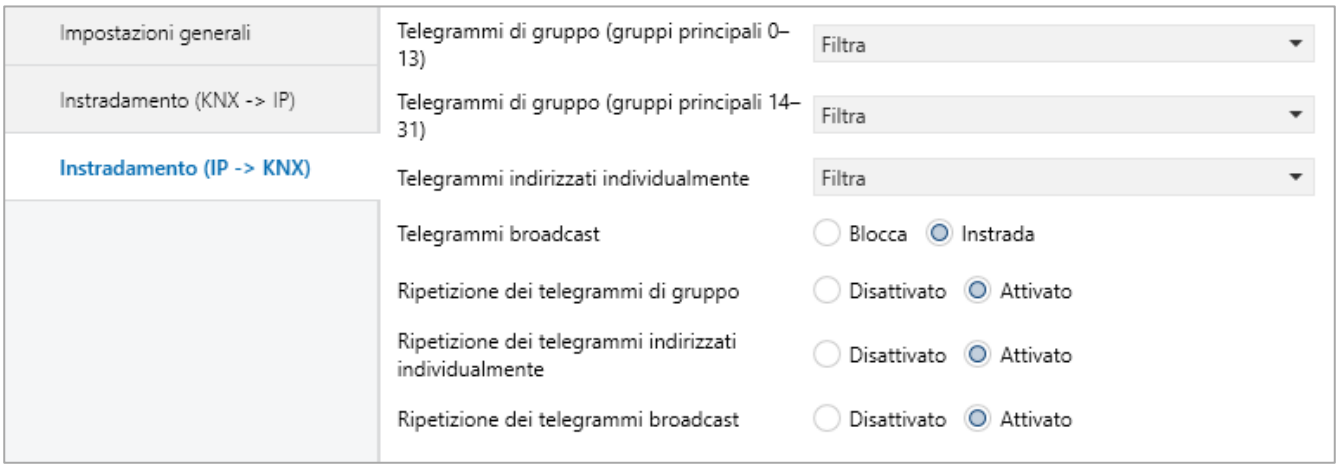
Sempre: Viene generato un riconoscimento per ogni telegramma indirizzato individualmente ricevuto (da KNX).

Solo se instradato: Viene generato un riconoscimento solo per i telegrammi di gruppo indirizzati individualmente ricevuti (da KNX) se questi vengono instradati all'IP.

Rispondi con NACK: Ogni telegramma indirizzato individualmente ricevuto (da KNX) riceve una risposta NACK (Not acknowledge). Ciò significa che la comunicazione con telegrammi indirizzati individualmente sulla linea KNX corrispondente non è possibile. La comunicazione di gruppo (telegrammi di gruppo) non è interessata. Questa impostazione può essere utilizzata per bloccare i tentativi di manipolazione.

Quando si utilizza “Rispondi con NACK”, l'accesso al dispositivo tramite KNX TP non è più possibile. La configurazione deve essere eseguita tramite IP.

10 Instradamento (IP -> KNX)



Telegrammi di gruppo (gruppo principale da 0 a 13)

Blocca: Nessun telegramma di gruppo di questi gruppi principali viene instradato a KNX.

Instrada: Tutti i telegrammi di gruppo di questo gruppo principale vengono instradati a KNXG indipendentemente dalla tabella dei filtri. Questa impostazione viene utilizzata solo a scopo di test.

Filtra: La tabella dei filtri viene utilizzata per verificare se il telegramma di gruppo ricevuto deve essere instradato a KNX.

Telegrammi di gruppo (gruppo principale da 14 a 31)

Blocca: Nessun telegramma di gruppo dei gruppi principali da 14 a 31 viene instradato a KNX.

Instrada: Tutti i telegrammi di gruppo dei gruppi principali da 14 a 31 vengono instradati a KNX.

Filtra: La tabella dei filtri viene utilizzata per verificare se il telegramma di gruppo ricevuto deve essere instradato a KNX.

Telegrammi indirizzati individualmente

Blocca: Nessun telegramma indirizzato individualmente viene instradato a KNX.

Instrada: Tutti i telegrammi indirizzati individualmente vengono instradati a KNX.

Filtra: L'indirizzo individuale viene utilizzato per verificare se il telegramma indirizzato individualmente ricevuto deve essere instradato a KNX.

Telegrammi broadcast

Blocca: Nessun telegramma broadcast ricevuto viene inoltrato a KNX.

Instrada: Tutti i telegrammi broadcast ricevuti vengono inoltrati a KNX.

Ripetizione dei telegrammi di gruppo

Disattivato: Il telegramma di gruppo ricevuto non viene reinviato a KNX in caso di guasto.

Attivato: Il telegramma di gruppo ricevuto viene reinviato fino a tre volte in caso di guasto.

Ripetizione dei telegrammi indirizzati individualmente

Disattivato: Il telegramma indirizzato individualmente ricevuto non viene reinviato a KNX in caso di guasto.

Attivato: Il telegramma indirizzato individualmente ricevuto viene reinviato fino a tre volte in caso di guasto.

Ripetizione dei telegrammi broadcast

Disattivato: Il telegramma broadcast ricevuto non viene reinviato a KNX in caso di guasto.

Attivato: Il telegramma broadcast ricevuto viene reinviato fino a tre volte in caso di guasto.

11 Programmazione

Il dispositivo può essere programmato in diversi modi tramite ETS:

Tramite bus KNX

Il dispositivo deve essere collegato solo al bus KNX. ETS richiede un'interfaccia aggiuntiva (ad esempio USB) per avere accesso al bus. In questo modo è possibile programmare sia l'indirizzo individuale che l'intera applicazione, compresa la configurazione IP. La programmazione tramite bus è consigliata se non è possibile stabilire una connessione IP.

Tramite KNXnet/IP Tunneling

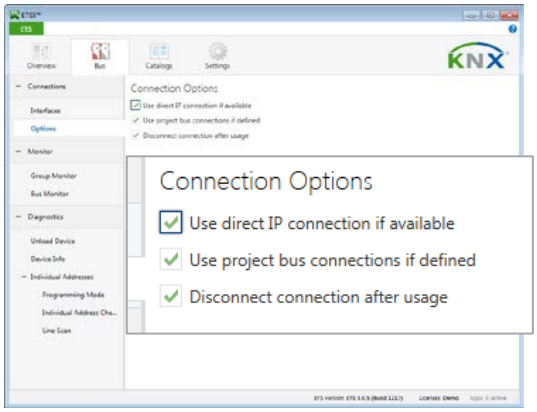
Non è necessaria alcuna interfaccia aggiuntiva. La programmazione tramite KNXnet/IP Tunneling è possibile se il dispositivo dispone già di una configurazione IP valida (ad esempio tramite DHCP). In questo caso il dispositivo viene visualizzato nella configurazione dell'interfaccia dell'ETS e deve essere selezionato. Il download viene eseguito tramite il progetto ETS come per molti altri dispositivi.

Tramite KNXnet/IP Routing

La programmazione tramite KNXnet/IP Routing è possibile se il dispositivo dispone già di una configurazione IP valida (ad es. tramite DHCP o Auto IP). Nell'ETS, l'interfaccia di routing appare se è disponibile almeno un dispositivo sulla rete che supporta il routing. Il nome dell'interfaccia di rete appare nel PC come descrizione. Se il routing è selezionato come interfaccia, la programmazione viene eseguita dal progetto ETS come per gli altri dispositivi. In questo caso la LAN viene utilizzata come mezzo KNX come TP. Non è necessario alcun dispositivo di interfaccia aggiuntivo.

Tramite connessione IP diretta

Mentre KNXnet/IP Tunneling e KNXnet/IP Routing sono limitati alla velocità di KNX TP, il dispositivo può essere caricato tramite una connessione IP diretta ad alta velocità. La connessione IP diretta è possibile se il dispositivo dispone già di una configurazione IP valida e di un indirizzo individuale. A tal fine, selezionare “Utilizza connessione IP diretta se disponibile” nel menu ETS “Bus – Connessioni - Opzioni”. Il download viene quindi eseguito direttamente nel dispositivo e non è visibile nel monitor di gruppo ETS.



A causa dei tempi di trasmissione notevolmente più brevi, si consiglia di eseguire i download tramite IP.

Open Source Licenses

This product contains open source software license:

curve25519-donna: Curve25519 elliptic curve, public key function

Source: http://code.google.com/p/curve25519-donna/

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

code 70207147

LAST REVISION 01/2026

Punto di contatto indicato in adempimento ai fini delle direttive e regolamenti UE applicabili:
Contact details according to the relevant European Directives and Regulations:
GEWISS S.p.A. Via D.Bosatelli, 1 IT-24069 Cenate Sotto (BG) Italy tel: +39 035 946 111 E-mail: qualitymarks@gewiss.com

According to applicable UK regulations, the company responsible for placing the goods in UK market is:
GEWISS UK LTD - Unity House, Compass Point Business Park, 9 Stocks Bridge Way, ST IVES Cambridgeshire, PE27 5JL, United Kingdom tel: +44 1954 712757 E-mail: gewiss-uk@gewiss.com

+39 035 946 111
8:30 - 12:30 / 14:00 - 18:00
lunedì - venerdì / monday - friday

www.gewiss.com